ABSTRACT OF THE DISCLOSURE

The threat probability of events generated by a security device on a computer network is assessed by comparing the threat probability to a global threat probability. An abstract data type is used to describe how the events are combined to form a threat. If an event matches an unpopulated member of an instance of an abstract data type, the event is added to the instance and the probability of the instance is computed. If the probability of the instance is greater than a global threat probability, a dynamic threat assessment event is generated. A system for dynamically assessing threats to computers and computer networks system includes at least one security device that generates events, an event collection database, policy configuration information, and a dynamic threat assessment engine.